

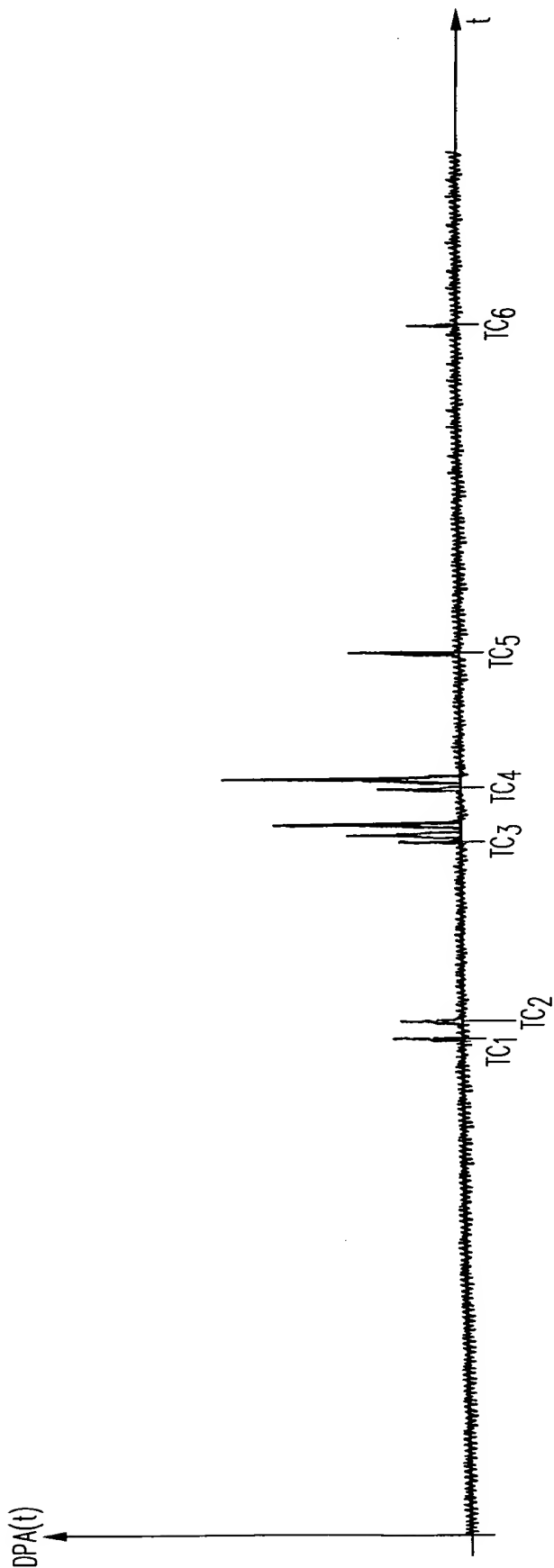


APPLN. FILING DATE: JULY 13, 2001  
TITLE: COUNTERMEASURE METHOD IN AN ELECTRONIC  
COMPONENT USING A SECRET KEY CRYPTOGRAPHIC  
ALGORITHM  
INVENTOR(S): CHRISTOPHE CLAVIER ET AL.  
APPLN. NO.: 09/807,615

SHEET 1 OF 13

1/13

FIG. 1



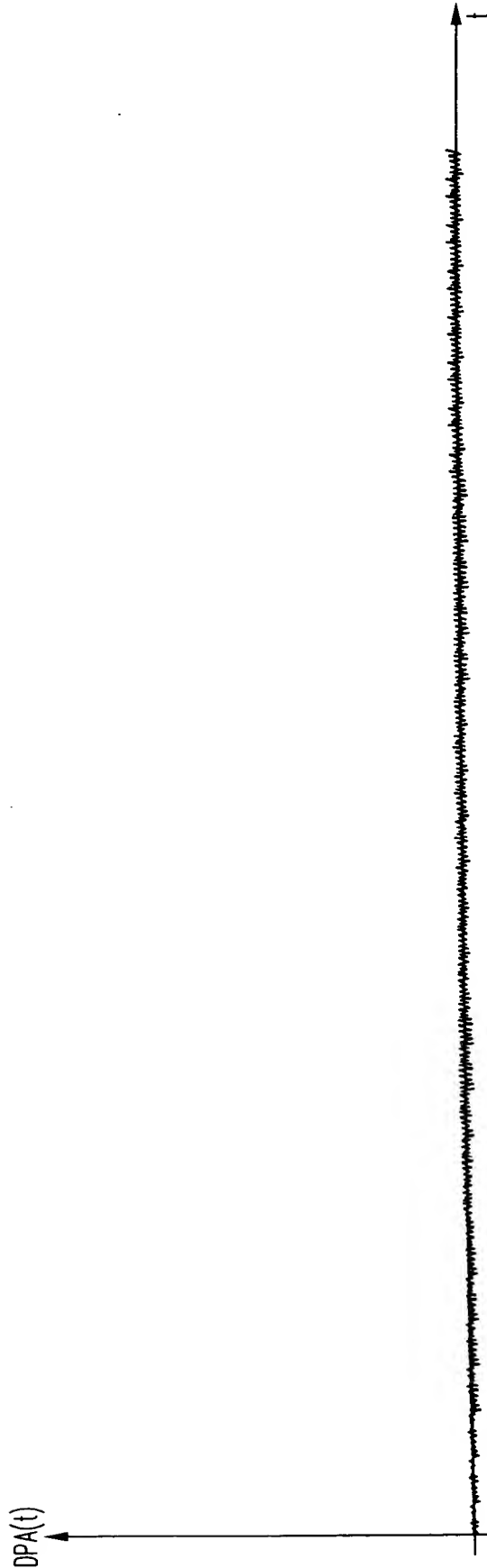


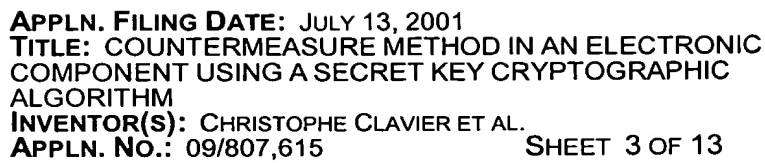
APPLN. FILING DATE: JULY 13, 2001  
TITLE: COUNTERMEASURE METHOD IN AN ELECTRONIC  
COMPONENT USING A SECRET KEY CRYPTOGRAPHIC  
ALGORITHM  
INVENTOR(S): CHRISTOPHE CLAVIER ET AL.  
APPLN. No.: 09/807,615

SHEET 2 OF 13

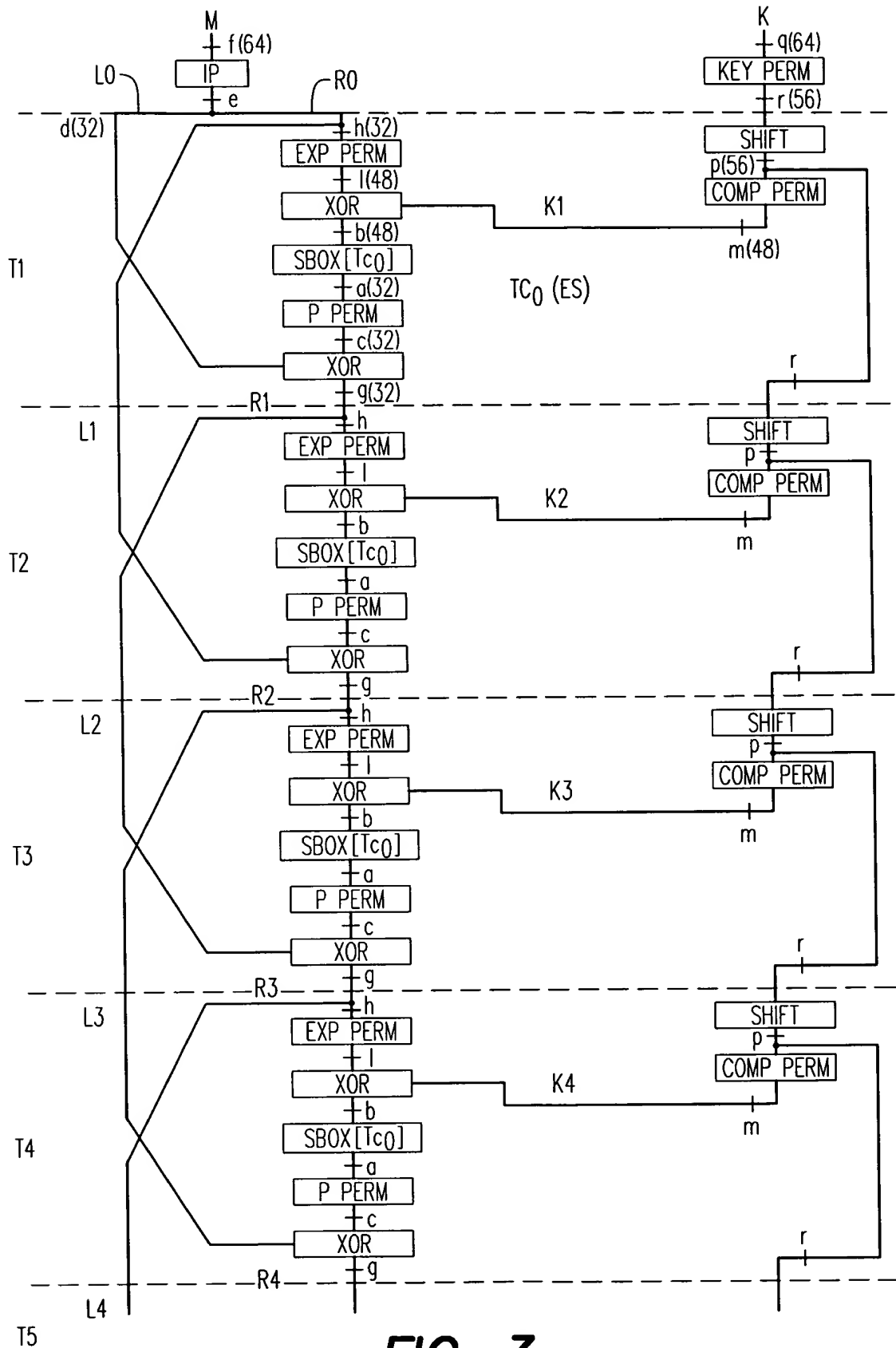
2/13

FIG. 2





**SHEET 3 OF 13**



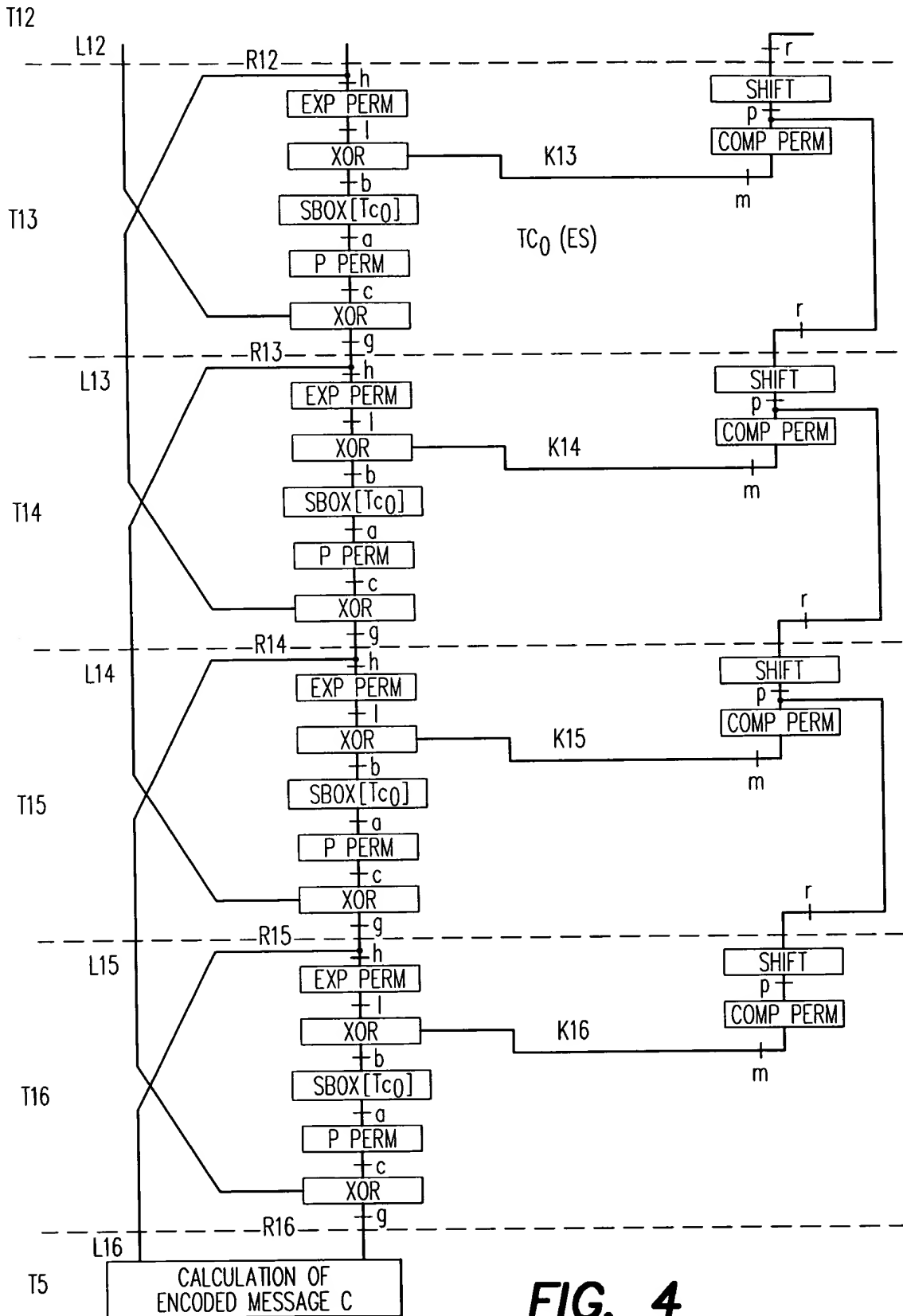
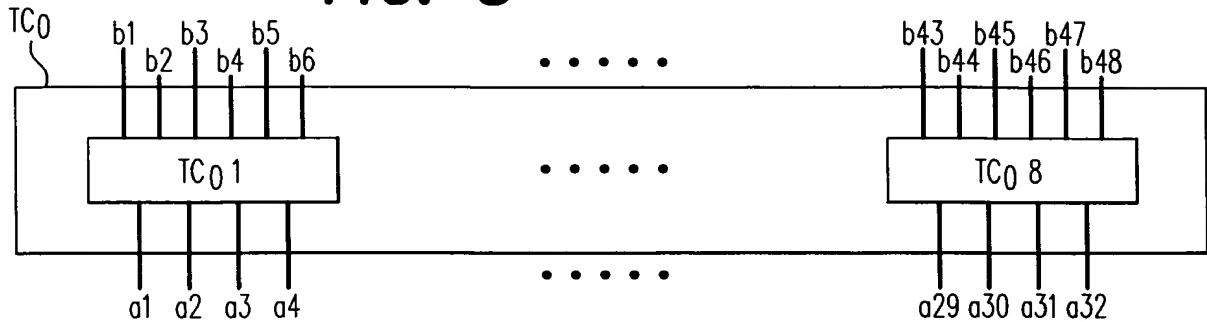


FIG. 4



**FIG. 5**



**FIG. 6**

TC<sub>0</sub> 1

$E = b_1b_2b_3b_4b_5b_6$	$S = a_1a_2a_3a_4$
000000	1101
000001	0101
⋮	⋮
111111	1010

**FIG. 10**

TC<sub>1</sub> 1

$E = b_1b_2b_3b_4b_5b_6$	$\overline{S} = \overline{a_1a_2a_3a_4}$
000000	0010
000001	1010
⋮	⋮
111111	0101

**FIG. 9**

TC<sub>2</sub> 1

$\overline{E} = \overline{b_1b_2b_3b_4b_5b_6}$	$\overline{S} = \overline{a_1a_2a_3a_4}$
000000	0101
⋮	⋮
111110	1010
111111	0010

**FIG. 16**

TC<sub>3</sub> 1

$\overline{E} = \overline{b_1b_2b_3b_4b_5b_6}$	$S = a_1a_2a_3a_4$
000000	1010
⋮	⋮
111110	0101
111111	1101

**FIG. 18**

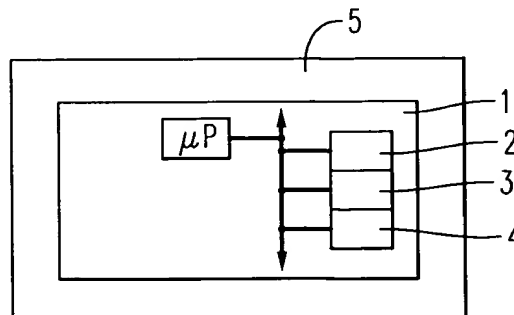
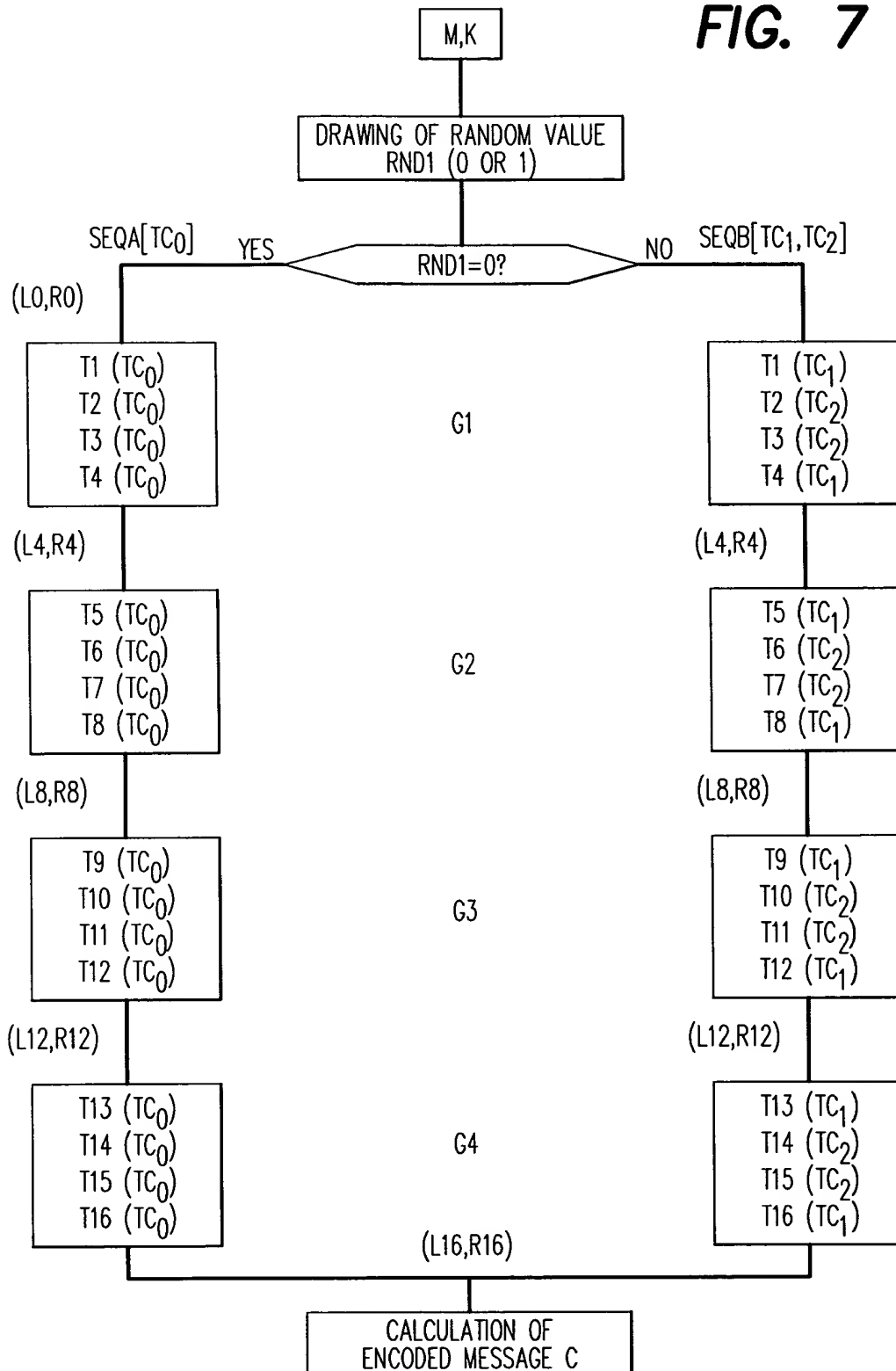




FIG. 7



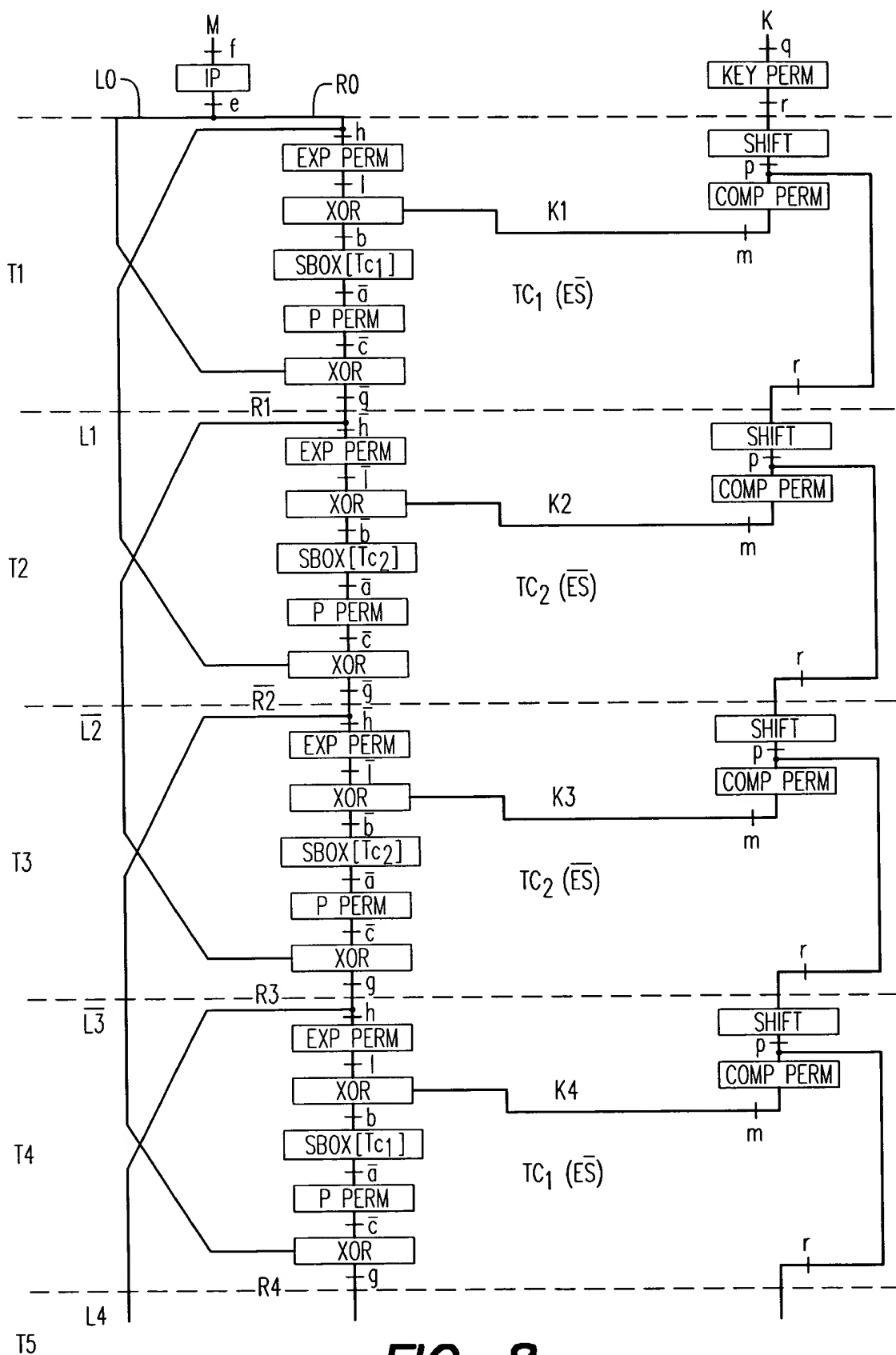
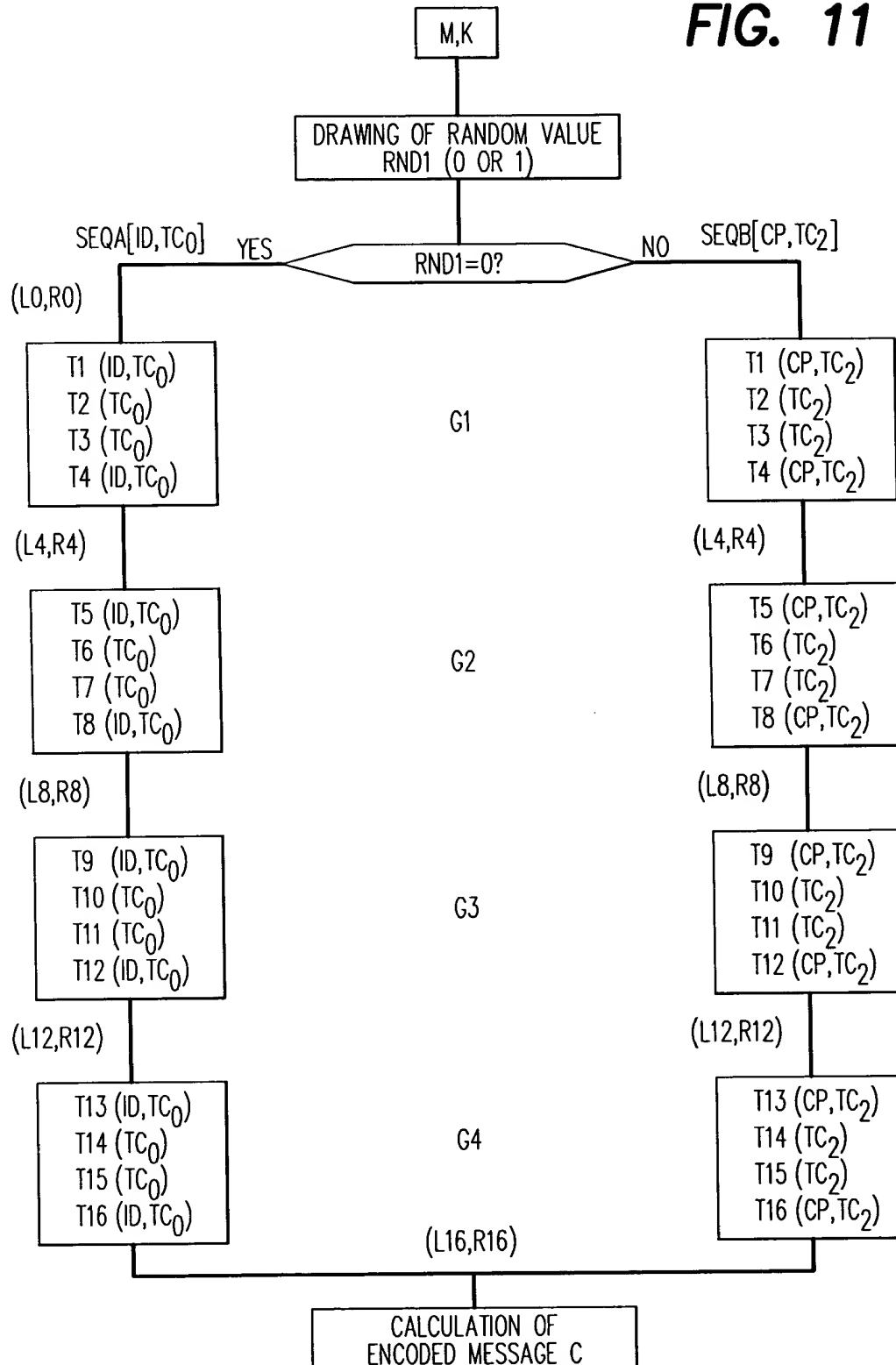


FIG. 8



FIG. 11







9/13

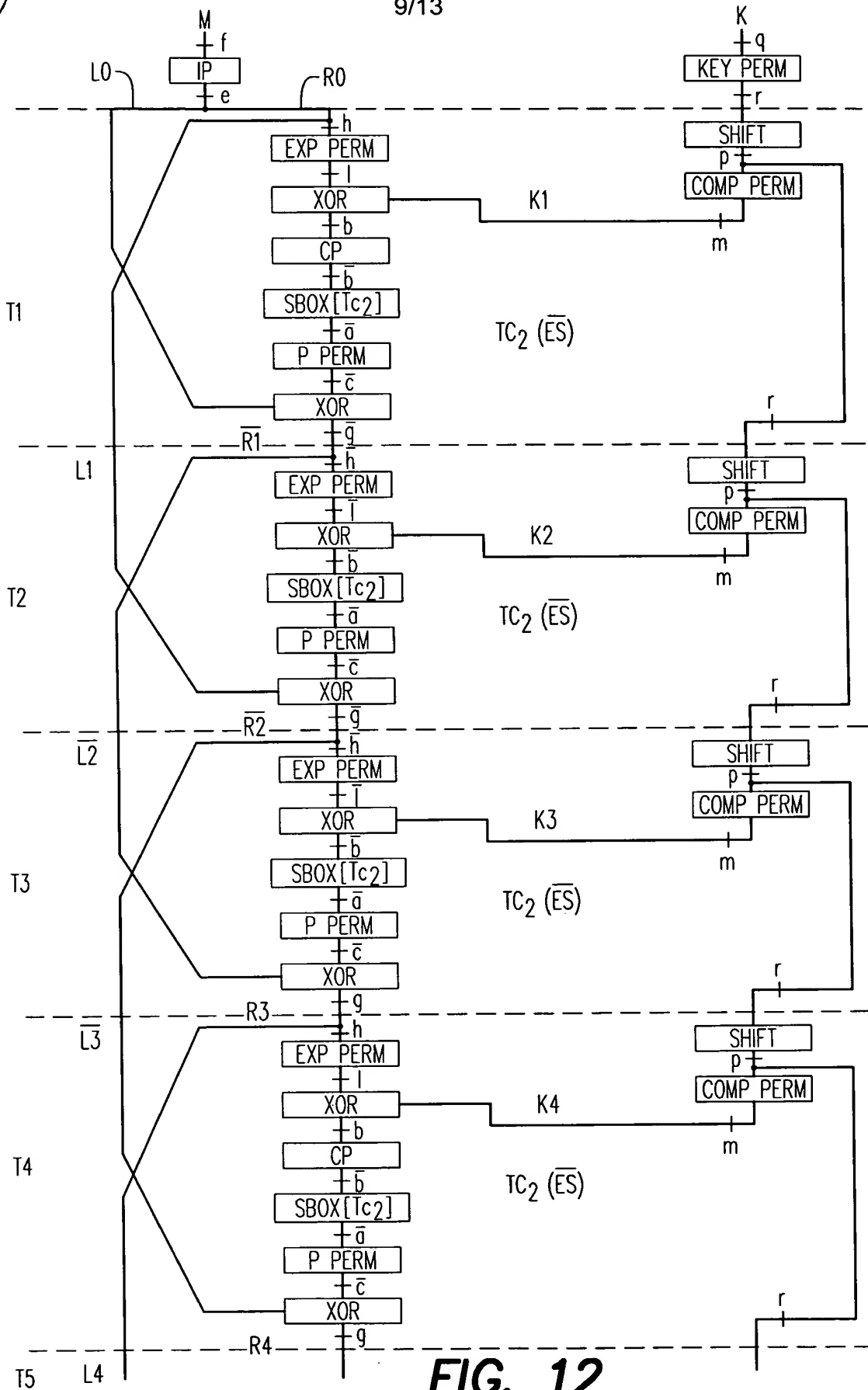
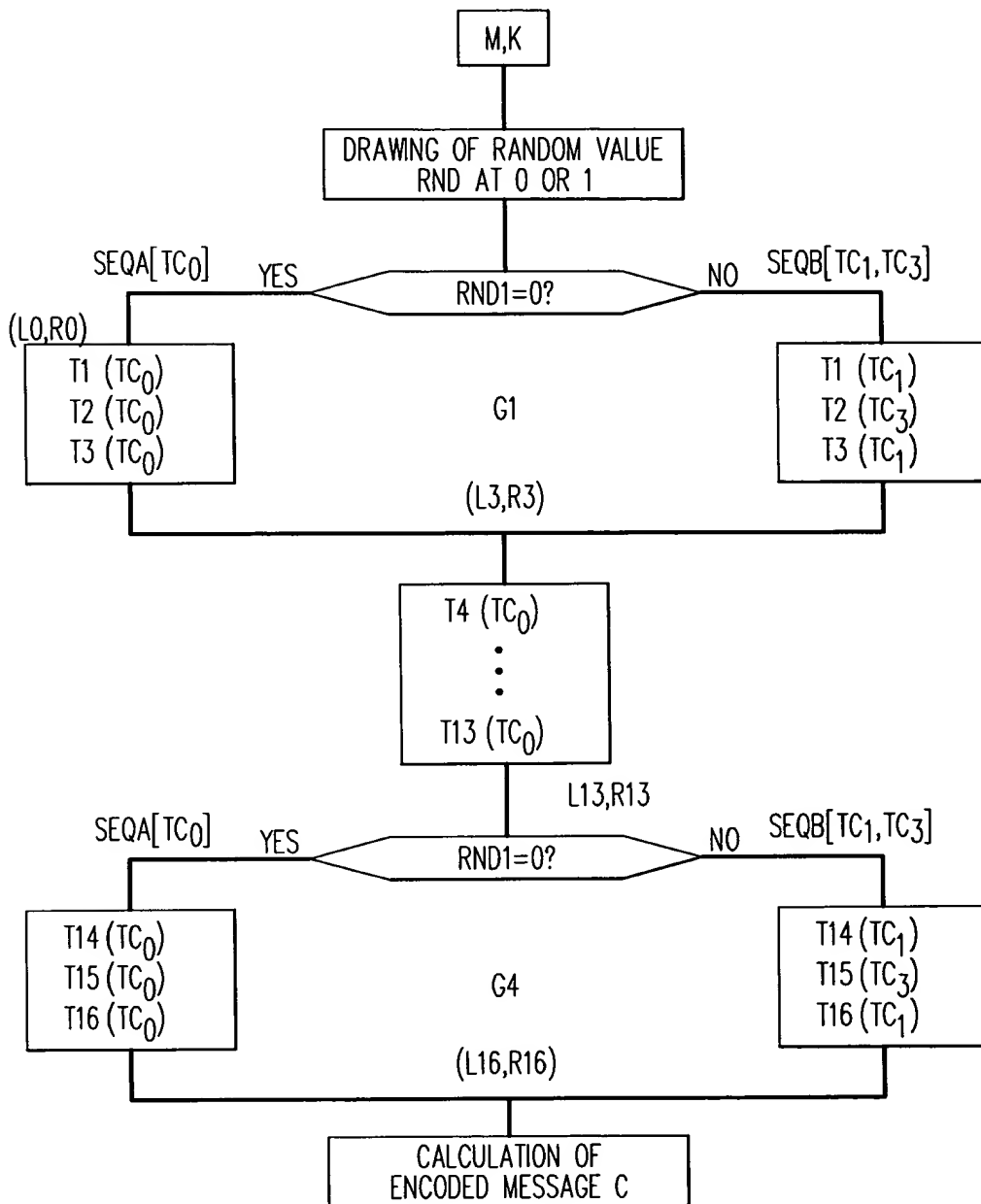


FIG. 12



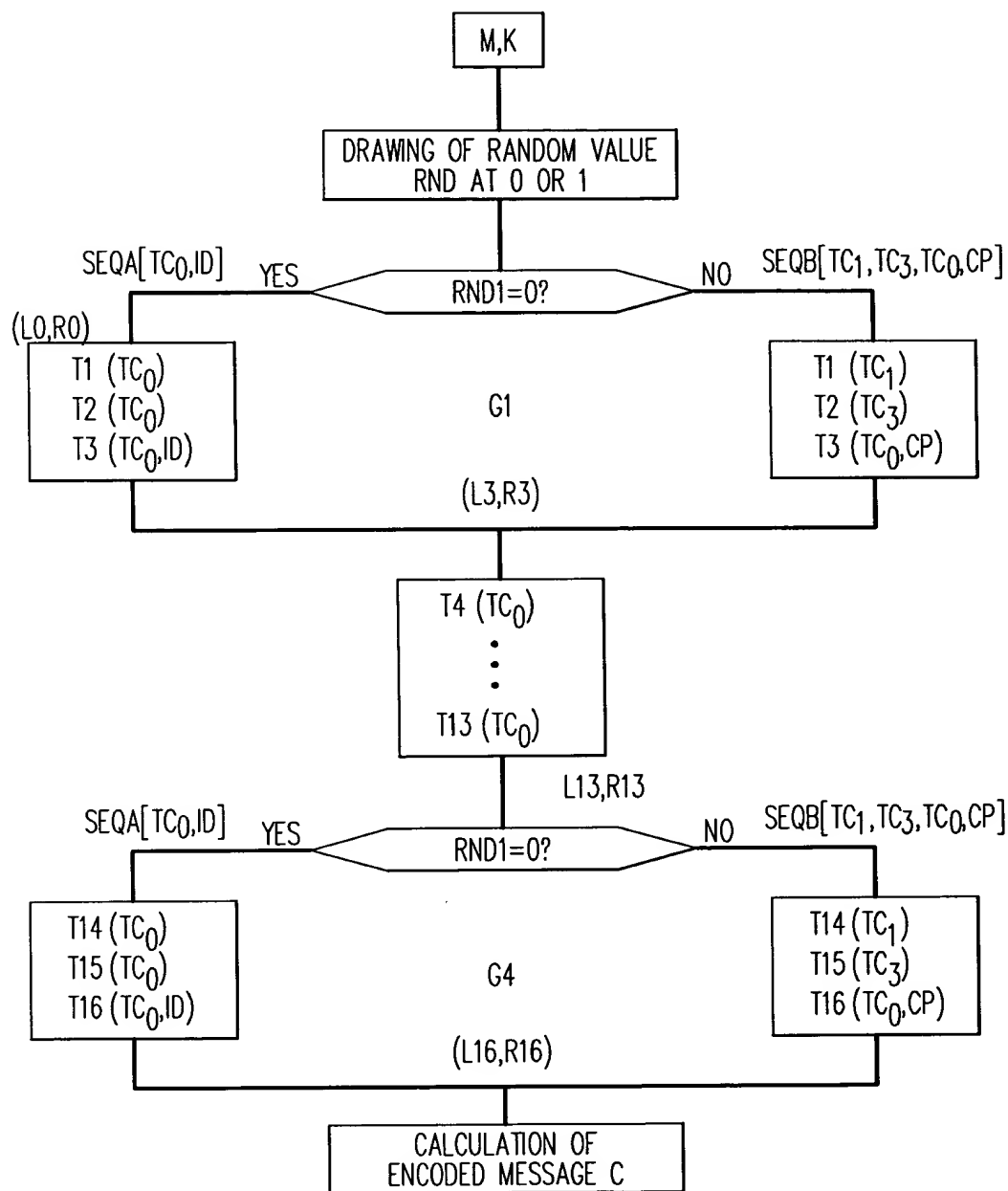


**FIG. 14**





13/13



**FIG. 17**